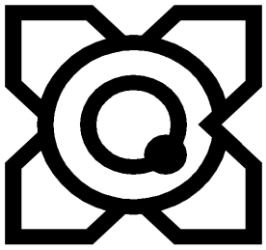
兴原认证中心良好认证审核案例



案例名称：北京奥特美克科技股份有限公司审核案例

案例序号： 01

案例类型： 体系认证

涉及体系： ISMS

审核类型： 初次审核

编 写 人： 李华

兴原认证中心有限公司

2019 年 3 月 25 日

地址：北京市海淀区上地三街 9 号嘉华大厦 C 座 711 邮政编码：100085

联系人：项兰倩 电话：010-62983830 手机：15210565296 邮箱:xqcc3@163.com

目 录 清 单

关于开展2019年度良好认证审核案例同行评议交流活动暨第一届认证技术交流研讨会的工作报告

中国认证认可协会自律监管部：

一、非常感谢中国认证认可协会对我中心2018年度良好认证审核活动的大力支持。2018年我中心上报认证认可协会16个案例，其中2个案例入选协会评议交流活动，今年我中心将再接再厉，争取能取得更大的成绩。

二、我中心积极响应认证认可协会举办的2019年度良好认证审核案例同行评议交流系列活动暨第一届认证技术交流研讨会，具体工作汇报如下：

1、自接到协会开展2019年度良好认证审核案例评议交流活动暨第一届认证技术交流研讨会的通知（中认协行〔2018〕255号文件）后，中心领导非常重视，成立了以总工为组长的良好认证审核案例工作小组，研究和部署了我中心2019年度良好认证审核案例征集流程、评定办法、推选和制定审核员提交良好审核案例的激励机制。

2、2019年01月07日通过中心信息平台向所有审核员发布征集案例通知，并得到各审核员的积极响应。

3、截止到2019年02月24日，我们共收到审核员提交的良好认证审核案例共计67个，安排专人负责整理所提交的案例。

4、2019年02月25日发给中心每位审核员（含实习）进行网络评议，共收到网络评议打分表166份，案例工作小组根据各审核员的网络评

议打分进行汇总统计，选出28个案例（即平均得分前28名的案例）作为初评案例，参加中心现场评议交流活动。

5、2019年03月18日在中心会议室，组织召开了初评案例的现场评议交流活动，参加案例评议活动的评委有副总经理（管理者代表）、相关部门负责人、认证决定人员以及案例编写人员，通过大家现场评议评选出12个兴原认证中心2019年度优秀认证审核案例。

6、2019年03月21日，对良好案例进一步修订和完善，并装订成册报送中国认证认可协会。

三、连续几年来，我中心在认证认可协会的组织领导下，以开展良好认证审核案例为抓手，加强审核员队伍水平建设，进一步提高认证审核工作的规范性和有效性，提升认证服务质量，为中国认证认可事业“传递信任、服务发展”做出积极贡献。

再次感谢认证认可协会长期以来对我中心工作的支持和帮助！

兴原认证中心有限公司

2019 年 03 月 25 日

认证技术交流研讨材料/良好认证案例推荐表

<table>
<tr><td>推荐机构名称
（盖章）</td><td colspan="3">兴原认证中心有限公司</td></tr>
<tr><td>获证组织名称</td><td colspan="3">北京奥特美克科技股份有限公司</td></tr>
<tr><td>案 例 类 型</td><td>质量管理升级版 □</td><td>产品认证 □</td><td>体系认证 ☑</td></tr>
<tr><td>认证人员姓名</td><td colspan="3">李华（组长）、秦佩君、王玉杰、高玉芝</td></tr>
<tr><td colspan="4">经验材料/案例特点简述及推荐意见(可加附页)</td></tr>
<tr><td colspan="4">1、充分关注了企业信息化产品开发、信息系统运行维护服务的特点：审核组基于资料收集、和企业沟通、现场查看等方式，多方位理解北京奥特美克科技股份有限公司主营的智慧水务、信息数据采集、水资源信息传输、末端采集产品研制、水环境项目规划和集成实施等业务过程。以期准确把握受审核企业的信息资产的种类、重要资产的分布、信息安全的薄弱点、项目现场控制措施的充分性。除了审核了本部的所有部门，还抽查了沧州市运河区水务局非农取水在线监控项目的集成和运维现场。
2、很好地把握了企业信息资产及其信息安全潜在风险的审核：审核组从电子数据和文档、纸质文档、硬件和设备、软件和系统、岗位和人员、服务、无形资产等方面审查了受审核企业资产识别的充分性，验证了重要资产分析时考虑了运维人员账密、实习生、仪表检验数据、现场备附件等方面，在面临的网络攻击、传输网络异常、越权访问、风险意识低等威胁时，可能发生的系统破坏、无法访问、数据丢失等信息安全事件，并将 43 项高风险结合企业的业务活动进行了核查。
3、帮助受审企业较为明显地改进了信息安全重大风险的识别和管理：审核组核查了资产管理、访问控制、物理和环境管理、运行管理、通信安全、系统获取开发和维护、供应商管理、业务连续性管理中的信息安全、符合性。无人值守计算机文件清理、移动介质登记使用、日志信息的追溯性、设备接电实况记录完整性等方面，提出了 7 个不符合项和 15 项书面观察项，促进了企业纠正和改进。</td></tr>
<tr><td colspan="4">证明及简述材料(可加附页)</td></tr>
<tr><td colspan="4">材料清单：■审核计划
■不合格项
■改进措施及企业整改成效证明</td></tr>
</table>

北京奥特美克科技股份有限公司信息安全管理体系初次审核案例

——围绕业务活动深入识别企业的信息安全风险

兴原认证中心有限公司　　李　华

1 案例背景

1.1 认证领域和类型：信息安全管理体系初次审核，认证范围为：与数据信息采集系统软、硬件的设计、开发和服务；系统集成项目的设计、实施和服务活动相关的信息安全管理活动，专业代码为：04.08（信息与通信技术）（中风险）。

1.2 审核日期及审核组：

1) 2018 年 5 月 14 日至 2018 年 5 月 15 日，一阶段审核，审核组：李华（组长）、秦佩君。
2) 2018 年 6 月 4 日至 2018 年 6 月 5 日，二阶段审核，审核组：李华（组长）、秦佩君、王玉杰、高玉芝。
3) 2018 年 6 月 15 日，二阶段项目现场审核，审核组：李华（组长）。

CNAS 派出评审组对二阶段审核组的认证审核能力进行了全程见证。

1.3 受审核方情况：北京奥特美克科技股份有限公司，2000 年成立，位于北京市海淀区西北旺东路 10 号院中关村软件园二期互联网创新中心 601。公司主营智慧水务、信息数据采集、传输、规划设计、产品提供、项目集成和实施等。以水环境、水安全、水生态、水经济为主线，利用大数据、云计算、物联网、移动互联等技术，构建智慧水务“云+端”及“涉水大数据应用服务平台”，形成了覆盖规划设计、咨询评估、软硬件产品研制、运维服务于一体的经营模式，已有数十万台/套产品在水利、农业、环保、海洋、住建等行业中得到应用，2017 年总设备 3 万多套，分布在 29 个省市自治区、299 个区县水务监控现场。

本次审核覆盖的部门包括：管理层、研发中心、供应链中心、客服中心、行政人事中心、财务中心、沧州市运河区水务局非农取水在线监控采购项目。

1.4 审核预期目的：证实受审核方信息安全管理体系与审核准则的符合性及有效性，确定是否推荐认证。本次审核结论是：不符合项书面验证合格后，管理体系符合性和有效性满足适用要求，具有实现预期结果的能力，审核组推荐认证。

1.5 认证依据包括：GB/T22080-2016 idt ISO/IEC27001:2013 信息安全管理体系 要求、信息安全管理手册 V1.1、适用性声明 V1.1 等。

2 审核过程

2.1 审查了管理体系文件策划

审查该公司依据 GB/T22080-2016 idt ISO/IEC27001:2013 的要求建立和运行管理体系的总体情况。公司编制了四级管理体系文件，一级：信息安全管理手册、适用性声明。二级：程序文件包括：文件控制程序、记录控制程序、信息安全和 IT 服务职能说明、信息安全和信息技术服务管理评审程序、资产识别和信息安全风险管理程序、介质和信息交换管理程序、用户访问管理程序、信息系统获取开发与维护管理安全管理程序、涉密信息的分析处理管理程序、防病毒管理程序、日志管理程序、信息备份管理程序、信息安全事件管理程序等。三级：工作流程，包含 2018 年运营管控体系、奥特美克部门职责说明书等 42 个。四级：记录表单，包括信息资产识别表、重大风险处置计划、各部门运行证据等记录表单。层次结构合理、内容符合一致性要求。

2.2 审查了信息资产识别和风险评价的结果

审核组查看了信息资产识别和风险评价，并与公司实际运行证据相比对。信息资产识别的类别包括：电子数据和文档、纸质文档、硬件和设备、软件和系统、岗位和人员、服务、无形资产。信息密级分类为 3 类：公司秘密（内部公开）、公司机密、公司绝密。对信息资产的保密性、完整性和可用性的赋值等级分为 5 级，5 级极高、1 级可忽略。

查见信息安全管理小组编写的 2017 年 10 月 31《JL-CX06-04 信息安全风险评估报告》，描述了《信息资产识别表》，共识别资产 484 项；对于资产值大于等于 3 的做为重要信息资产，形成了《重要资产清单》。重要资产共：191 项。针对重要资产各部门又对其威胁、脆弱性进行了分析，基于现有的控制措施实施风险评估后确定了风险值，风险值大于等于 3 的为高风险，确定的高风险数为 43 项。公司随后针对这 43 项高风险制定了“风险处置计划”，处置计划实施完成后又进行了二次评估。经风险处置后，所有风险都降到了最低。

2.3 审查了重要控制域的管理要求及其落实情况

审核组按照适用性声明中描述的控制措施，核查了如下方面的管理策划和实施：资产管理、访问控制、物理和环境管理、运行管理、通信安全、系统获取开发和维护、供应商管理、业务连续性管理中的信息安全、符合性。收集到大量符合性证据。

2.4 审查了项目管理中的信息安全

审核组按照审核计划，抽查了智能雷达水位计项目资料、“县级山洪完善项目”软件开发项目实施证据、沧州市运河区税务非农取水在线监控采购项目现场。

在沧州项目现场，（a）查看了数据采集终端设备《检测报告》（b）现场访谈甲方负责人，了解了水务局的保密和数据管理要求。巡视了东水厂（第 3 个现场）。（c）了解到项目资料在水务及局有专门的资料柜、设备有专门库房暂存。登录水务局用户查看了系统授权和数据管理情况。

3 主要的审核发现、沟通过程

3.1 不符合项事实

审核组根据审核发现，共提出 7 个不符合项和 15 项书面观察项。其中不符合项涉及的部门和条款是：体系管理小组：A.11.2.9；财务中心：A.8.3.1；研发中心：A.9.2.2/A.9.2.3/A.9.2.5；行政人事中心：A.12.4.3、A.12.4.4；质量管理部： A.11.2.8; 客服中心：A.6.1.5。

本案例重点介绍如下 4 个不符合项和沧州项目现场的 2 个书面观察项：

第 1 项不符合（轻微不符合）：现场查公司第一会议室笔记本电脑（ZL-33）和公司培训室台式计算机（ZL-38），未设开机密码、无屏保。两台机器中都有部门技术资料和会议记录等。

以上事实不符合 GB/T22080-2016 idt ISO/IEC27001:2013 标准 A.11.2.9 条款的相关要求。

第 2 项不符合（轻微不符合）：查见公司对 U 盘发放建立了办公用品发放记录，但对于使用去向追溯（比如投标交付）和使用情况缺少管理证据。

现场查见 2018 年 3 月 13 日吕*领取 1 个 2G 容量优盘。2018-6-5 上午已用 1.48G。存储了从 2017 年至今的公司财务文件，包括经营情况表、预算表等。吕说该优盘放在他的随身包中，经常在家办公需要使用。查公司 OA 系统《可移动介质授权审批表》，未见吕*U 盘记录。

以上事实不符合 GB/T22080-2016 idt ISO/IEC27001:2013 标准 A.8.3.1 条款的相关要求。不符合《AMCX08 介质和信息交换管理程序》关于“向可移动介质拷贝涉密信息，或将可移动介质带离开本公司需要获得本部门领导的批准，并在《可移动介质授权使用清单》上记录存储的信息、用途、批准人、操作人等相关信息”的管理规定。

第 4 项不符合（轻微不符合）：查《AMCX16 日志管理程序》对日志定期评审没有规定。门禁系统日志管理员可以删除日志信息。

以上事实不符合 GB/T22080-2016 idt ISO/IEC27001:2013 标准 A.12.4.3 条款的相关要求。

第 7 项不符合（轻微不符合）：客服中心租用上海新道仓信息科技有限公司开发 SaaS（软件即服务）平台类软件“北京奥特美克运维服务管理系统”，用于运维项目管理。对其数据存放地理位置、安全防护措施未做明确要求；现场登录系统，发现工单上有客户的姓名和联系电话等敏感信息显示，未见识别和防护证据。

以上事实不符合 GB/T22080-2016 idt ISO/IEC27001:2013 标准附录 A 中 A.6.1.5 条款的相关要求。

沧州项目现场的 2 项书面观察项：

（1）应关注《施工组织方案》项目人员岗位职责中信息安全管理内容的完善性，并在施工安全文明交底中强调信息安全管理要求。

（2）现场查看到，在 3 个设备安装现场均看到 220 伏市电供电不连接，建议在施工日志或安装调试记录中记录该类实际情况。

3.2 不符合项沟通

审核组在现场和公司总经理及相关部门人员对不符合项进行了有效沟通，解释了信息资产及其风险控制对公司业务安全的影响，说明了目前的不符合情况宜抓紧整改，以防范潜在的不利影响。

经过沟通，审核组提出的不符合项得到受审核方人员的理解和接受。

3.3 企业整改

第 1 项不符合：对该台会议室电脑中的会议资料进行了清理，设置了关机清理功能。企业对共用电脑进行了检查，设置了必要的开机密码屏保。

第 2 项不符合：公司完善了移动介质领用审批。对 U 盘进行统一检查和清理。

第 4 项不符合：修订了日志管理程序，补充了监控系统的日志审核。

第 7 项不符合：和服务方签订了保密协议，明确了数据定期备份的要求。在资产识别表中增加了客户信息等要素。

4 受审核组织主要的改进方法及其成效

受审核方首先针对审核组提出的不符合项进行了纠正，提供了相关的证据。

公司 2018-6-8 组织培训，宣贯了不符合项纠正措施涉及的内容。现场交流，确认大家了解了相关要求。公司 2018-6-20 在内网上发布了不符合项整改内容和书面观察项，请全员给以关注、认真学习、纠正问题、举一反三、持续改进。

通过整改，相关部门和岗位提高了信息安全风险意识，从技术手段上、和相关方协约上、移动介质使用、项目现场信息保护等方面，切实认识到与标准要求存在差距，为此公司建立了改进的有效措施，对提高公司业务信息的保密性、完整性和可用性，带来了明显的改进和效果。

本案例结合审核组上面描述的不符合和书面观察项，具体解释一下能帮助企业避免怎样的潜在风险：

第 1 项不符合事实的潜在风险：公司电脑在公司召开周例会、月工作会、高层研讨、项目论证过程中用于投影相关资料，资料的内容由较为敏感的信息，用于电脑是共用的、如果文件不及时清理，存在资料可能被超权限复制或浏览或泄露的风险。培训室的计算机保存了给实习生、客户培训的资料，为内部使用、含客户或项目的敏感信息，在没有开机密码屏保的情况下，容易被人利用复制敏感资料。

第 2 项不符合事实的潜在风险：移动介质的发放数量不清楚、领用无审批、去向不掌握，容易发生保存了敏感信息的 U 盘丢失、失控、信息泄露等。特别是财务主管保存了大量财务数据的 U 盘在随身携带、在家办公的情况下，存在发生意外丢失、被盗取、信息被复制等可能，财务数据的敏感性、保密性对上市公司应该是非常重要的。

第 4 项不符合事实的潜在风险：信息系统的日志如果不进行定期评审，有些异常情况（比如：异常访问、网络攻击、备份失效、应用服务停止等）可能不会及时发现。门禁系统日志可追溯人员进出、开通、撤销等活动，如果管理员可以删除日志信息，可能会被人利用删除敏感记录。

第 7 项不符合事实的潜在风险：服务提供方是否遵守信息安全管理要求，是否合理合规地管理企业数据，对企业的信息安全影响较大。很多事实表明，服务提供方管理薄弱，或者敏感信息不当地传递给了服务提供方，会导致信息泄露重大事件的发生。

沧州项目现场的 2 项书面观察项的潜在风险：（1）现场人员长期在外工作，公司总部的培训、会议等往往不能参加，这样信息安全管理的要求就需要有合适的途径结合项目工作进行传达和贯彻，审核组建议企业关注《施工组织方案》项目人员岗位职责中信息安全管理内容的完善性，并在施工安全文明交底中强调信息安全管理要求。（2）关于 3 个设备安装现场均看到 220 伏市电供电不连接的情况，因为企业产品说明中描述可 220 伏市电供电方式工作。实际中如果发生太阳能电池失效或其他异常情况，运维人员不了解无 220 伏市电连接，可能会错误理解系统运行状态。因此审核组建议在施工日志或安装调试记录中记录该类实际情况。

5 结束语

审核组在审核过程中，充分关注了企业信息化产品开发、信息系统运行维护服务的特点，结合标准要求，很好地把握了相关的信息资产及其信息安全潜在风险。通过本次信息安全管理体系初次审核，帮助受审企业较为明显地改进了信息安全重大风险的识别和管理。

附件：

审核计划

XQCCB207-1/2　　1997 年 10 月首次发布　　2016 年 7 月第 17 次修改

审 核 计 划

项目号：1801-0108-IS2　　■IS

受审核方名称	北京奥特美克科技股份有限公司		法人代表	吴 玉晓	联系人	王帅伟
地　　址	北京市海淀区西北旺东路 10 号院中关村软件园二期互联网创新中心 601				邮　编	100094
					email	690983695@qq.com
固定电话	010-82894254/55-8018、82894199	传真	010-82894252	审核日期	2018 年 6 月 4 日 上午至 2018 年 6 月 5 日 下午	
移动电话	18910728937　； 15010036119					
审核类型	IS：初审				方式	■ 单独 □ 联合
审核目的：■ 评价受审核方管理体系与认证依据标准的符合程度，确定是否推荐注册。						
审核范围（QMS 应说明不适用条款）： 与数据信息采集系统软、硬件的设计、开发和服务；系统集成项目的设计、实施和服务活动相关的信息安全管理活动；《适用性声明》（版本号：A/1）（边界：北京市海淀区西北旺东路 10 号院东区 5 号楼 6 层 601、602）***					专业小类代码： 04.08(中风险)	
审核准则： ■ISO/IEC27001:2013 ■受审核方管理体系文件的有效版本 ■适用的法律、法规、标准及其他要求						

审核组	姓 名	性 别	注册资格、专业	注册证书号	电　话	编号
组长	李华 H	女	审核员 04.08	2017-N1ISMS-1098579	13511017311 wzqis888@sina.com	A
组员	秦佩君	女	审核员 04.08	2017-N1ISMS-2017270	18611916022 pj_qin@sina.com	B
组员	王玉杰 H	女	见证审核员 04.08	2018-N1ISMS-2020948	13910051390 13910051390@163.com	C
组员	高玉芝 H	女	审核员 04.08	2016-N1ISMS-1216474	13521820840 2454265154@qq.com	D

备　注					
审核报告	分发范围：审核委托方/受审核方/兴原中心	预期分发时间	颁证/监督有效通知的同时	语言	汉 语
承　诺	在审核过程接触到的有关受审核方的一切机密信息，审核组全体成员有责任保守秘密，未经受审核方书面许可，不得向第三者泄露。				

审核组组长（签字）：	中心审核部意见：	受审核方代表意见：
李华 2018 年 5 月 18 日	签名：　　年 5 月 21 日	签名：　　年 6 月 4 日

审 核 计 划

项目号：1801-0108-IS2 ■IS

受审核方名称	北京奥特美克科技股份有限公司		法人代表	吴 玉晓	联系人	王帅伟
地 址	北京市海淀区西北旺东路 10 号院中关村软件园二期互联网创新中心 601			邮 编	100094
				email	690983695@qq.com
固定电话	010-82894254/55-8018、82894199	传真	010-82894252	审核日期	2018 年 6 月 4 日 上午至 2018 年 6 月 5 日 下午
移动电话	18910728937 ； 15010036119				
审核类型	IS：初审			方式	■ 单独 □ 联合

审核目的：■ 评价受审核方管理体系与认证依据标准的符合程度，确定是否推荐注册。

审核范围（QMS 应说明不适用条款）： 与数据信息采集系统软、硬件的设计、开发和服务；系统集成项目的设计、实施和服务活动相关的信息安全管理活动；《适用性声明》（版本号：A/1）（边界：北京市海淀区西北旺东路 10 号院东区 5 号楼 6 层 601、602）***	专业小类代码: 04.08(中风险)

审核准则：

■ISO/IEC27001:2013

■受审核方管理体系文件的有效版本

■适用的法律、法规、标准及其他要求

审核组	姓 名	性 别	注册资格、专业	注册证书号	电 话	编号
组长	李华 H	女	审核员 04.08	2017-N1ISMS-1098579	13511017311 wzqis888@sina.com	A
组员	秦佩君	女	审核员 04.08	2017-N1ISMS-2017270	18611916022 pj_qin@sina.com	B
组员	王玉杰 H	女	见证审核员 04.08	2018-N1ISMS-2020948	13910051390 13910051390@163.com	C
组员	高玉芝 H	女	审核员 04.08	2016-N1ISMS-1216474	13521820840 2454265154@qq.com	D

备 注					
审核报告	分发范围：审核委托方/受审核方/兴原中心	预期分发时间	颁证/监督有效通知的同时	语言	汉 语
承 诺	在审核过程接触到的有关受审核方的一切机密信息，审核组全体成员有责任保守秘密，未经受审核方书面许可，不得向第三者泄露。				

审核组组长（签字）： 李华 2018 年 5 月 18 日	中心审核部意见： 同意 (公章) 签名: 2018 年 5 月 21 日	受审核方代表意见： (公章) 签名: 年 月 日

项目号：1801-0108-IS2 ■IS

审核组内部沟通，6 月 4 日 8 时 00 分至 8 时 30 分，**请公司安排为审核组提供会议室**。									
首次会议 6 月 4 日 8 时 30 分至 9 时 00 分，受审核方管理层、各部门负责人参加。									
末次会议 6 月 5 日 16 时 30 分至 17 时 00 分，参加人员同首次会议。									
日期	时间	第 1 组（李华）		第 2 组（秦佩君）		第 3 组（王玉杰）		第 4 组（高玉芝）	
		受审核部门、主责条款	编号	受审核部门、主责条款	编号	受审核部门、主责条款	编号	受审核部门、主责条款	编号
6 月 4 日	9:00～12:30	**一阶段问题整改验证（9:00~10:00）** **管理层：IS：4.1、4.2、4.3、4.4、5.1、5.2、5.3、6.1、6.2、7.1、8.1、8.2、9.1、9.3、10.2、A.5.1.1、A.5.1.2、A.6.1.1、A.6.1.2、A.11.2.8、A.11.2.9、A.12.2.1、A.12.3.1、A.18.2.2;**	**A**	质量管理部：IS：通用条款、6.2、8.2、8.3、9.1、9.2、10.1、A.8.1.1、A.8.1.2、A.9.3.1、A.11.2.8、A.11.2.9、A.12.2.1、A.12.3.1；	B	供应链中心：IS：通用条款、8.2、8.3、A.8.1.1、A.8.1.2、A.9.3.1、A.11.2.8、A.11.2.9、A.12.2.1、A.12.3.1、A.15.1、A.15.1.1、A.15.1.2、A.15.1.3、A.15.2.1、A.15.2.2；	C	**行政人事中心：IS：通用条款、7.2、7.3、7.5、8.2、8.3、9.1、A.6.1.3、A.6.1.4、A.6.2.1、A.6.2.2、A.7.1.1、A.7.1.2、A.7.2.1、A.7.2.2、A.7.2.3、A.7.3.1、A.8.1.1、A.8.1.2、A.8.1.3、A.8.2.1、A.8.2.2、A.8.2.3、A.8.3.1、A.8.3.2、A.8.3.3、A.9.1.1、A.9.1.2、A.9.2.1、A.9.2.2、A.9.2.3、A.9.2.4、A.9.2.5、A.9.2.6、A.9.3.1、A.9.4.1、A.9.4.2、A.9.4.3、A.9.4.4、A.11、A.12.1.1、A.12.1.2、A.12.1.3、A.12.2.1、A.12.3.1、A.12.4.1、A.12.4.2、A.12.4.3、A.12.4.4、A.12.5.1、A.12.6.1、A.12.6.2、A.12.7.1、A.13.1.1、A.13.1.2、A.13.1.3、A.13.2.1、A.13.2.2、A.13.2.3、A.13.2.4、A.14.1.1、A.14.1.2、A.14.1.3、A.16.1.2、A.16.1.3、A.17.1、A.17.1.1、A.17.1.2、A.17.1.3、A.17.2.1、A.18.1.1、A.18.1.2、A.18.1.3、A.18.1.4、A.18.1.5;**	D
	13:00～17:00	体系管理小组：IS：7.4、8.1、8.2、A.8.1.3、A.11.2.8、A.11.2.9、A.12.2.1、A.12.3.1、A.16.1.1、A.16.1.4、A.16.1.5、A.16.1.6、A.16.1.7、A.18.2.1、A.18.2.3；	**A**	运营管理部：IS：通用条款、8.2、8.3、A.8.1.1、A.8.1.2、A.9.3.1、A.11.2.8、A.11.2.9、A.12.2.1、A.12.3.1；	B	**研发中心：IS：通用条款、8.2、8.3、A.6.1.5、A.8.1.1、A.8.1.2、A.9.2.1、A.9.2.2、A.9.2.3、A.9.2.4、A.9.2.5、A.9.2.6、A.9.3.1、A.9.4.3、A.9.4.4、A.9.4.5、A.11.2.8、A.11.2.9、A.12.1.4、A.12.2.1、A.12.3.1、A.14.2.1、A.14.2.2、A.14.2.3、A.14.2.4、A.14.2.5、A.14.2.6、A.14.2.8、A.14.2.9、A.14.3.1;**	C		D
	17:00～17:30	**审核组内部沟通**						**ABCD**	

日期	时间	第 1 组（李华）		第 2 组（秦佩君）		第 3 组（王玉杰）		第 4 组（高玉芝）	
		受审核部门、主责条款	编号	受审核部门、主责条款	编号	受审核部门、主责条款	编号	受审核部门、主责条款	编号
6 月 5 日	8:30～12:30	财务中心：IS：通用条款、8.2、8.3、A.8.1.1、A.8.1.2、A.9.2.1、A.9.2.2、A.9.2.3、A.9.2.4、A.9.2.5、A.9.2.6、A.9.3.1、A.9.4.3、A.9.4.4、A.10.1、A.10.1.1、A.10.1.2、A.11.2.8、A.11.2.9、A.12.2.1、A.12.3.1；	A	客服中心：IS：通用条款、8.2、8.3、A.6.1.5、A.8.1.1、A.8.1.2、A.9.3.1、A.11.2.8、A.11.2.9、A.12.2.1、A.12.3.1、A.18.1.1；	B	营销中心：IS：通用条款、5.3、8.2、8.3、A.8.1.1、A.8.1.2、A.9.3.1、A.11.2.8、A.11.2.9、A.12.2.1、A.12.3.1、A.18.1.1；	C	规划设计院：IS：通用条款、8.2、8.3、A.6.1.5、A.8.1.1、A.8.1.2、A.9.3.1、A.11.2.8、A.11.2.9、A.12.2.1、A.12.3.1；	D
	13:00～15:30	济源市水资源实时监控系统维护合同项目资料（数据处理）：IS：A.6.1.1、A.6.1.5、A.8.1.1、A.9.1.1、A.11.2.5、A.11.2.6、A.11.2.9、A.12.3.1、A.14、A.16.1.2、A.16.1.3、A.18.1.3；	A	广西山洪灾害防治县级监测系统恭城瑶族自治县售后服务合同项目资料（软件运维）：IS：A.6.1.1、A.6.1.5、A.8.1.1、A.9.1.1、A.11.2.5、A.11.2.6、A.11.2.9、A.12.3.1、A.14、A.16.1.2、A.16.1.3、A.18.1.3；	B	县级山洪完善项目资料（软件开发）：IS：A.6.1.1、A.6.1.5、A.8.1.1、A.9.1.1、A.11.2.5、A.11.2.6、A.11.2.9、A.12.3.1、A.14、A.16.1.2、A.16.1.3、A.18.1.3；	C	智能雷达水位计项目资料（硬件开发）：IS：A.6.1.1、A.6.1.5、A.8.1.1、A.9.1.1、A.11.2.5、A.11.2.6、A.11.2.9、A.12.3.1、A.14、A.16.1.2、A.16.1.3、A.18.1.3；	D
	15:30～16:00	补充审核、审核组内部沟通						**ABCD**	
	16:00～16:30	和管理层沟通						**ABCD**	

注：1）**通用条款（管理职责、安全需求、管理目标、沟通和改进情况）**在每个部门都应审核到，在审核计划中只需在主控部门列出即可(监督审核除外)。

2）对于监督/再认证审核：除本次正常审核的内容外，还要检查上次不符合项纠正措施的验证、认证证书及标志的使用情况、体系变更情况、对组织投诉记录的调阅、资质核查及再确认等。

3）本次审核验证情况：☐有 ☒无

4）其他事宜：无

审 核 计 划

项目号：1801-0108-IS2 ■IS

受审核方名称	北京奥特美克科技股份有限公司		法人代表	吴玉晓	联系人	王帅伟
地 址	北京市海淀区西北旺东路 10 号院中关村软件园二期互联网创新中心 601				邮 编	100094
					email	690983695@qq.com
固定电话	010-82894254/55-8018、82894199	传真	010-82894252	审核日期	2018 年 6 月 15 日 上午至 2018 年 6 月 15 日 下午	
移动电话	18910728937 ； 15010036119					
审核类型	IS：审核沧州的项目现场				方式	■ 单独 □ 联合
审核目的：■ 查看项目现场情况。						
审核范围（QMS 应说明不适用条款）： IS：与数据信息采集系统软、硬件的设计、开发和服务；系统集成项目的设计、实施和服务活动相关的信息安全管理活动；《适用性声明》（版本号：A/1）（边界：北京市海淀区西北旺东路 10 号院东区 5 号楼 6 层 601、602）***					专业小类代码： IS：04.08(中风险)	
审核准则： ■ISO/IEC27001:2013 ■受审核方管理体系文件的有效版本 ■适用的法律、法规、标准及其他要求						

审核组	姓名	性别	注册资格、专业	注册证书号	电话	编号
IS：组长	李华 H	女	IS：审核员 IS：04.08	IS：2017-N1ISMS-1098579	13511017311 wzqis888@sina.com	A
备 注						

审核报告	分发范围：审核委托方/受审核方/兴原中心	预期分发时间	颁证/监督有效通知的同时	语言	汉 语
承 诺	在审核过程接触到的有关受审核方的一切机密信息，审核组全体成员有责任保守秘密，未经受审核方书面许可，不得向第三者泄露。				

审核组组长（签字）： 李华 2018 年 5 月 18 日	中心审核部意见： 兴原认证中心有限公司 审核专用章 (公章) 签名：2018 年 06 月 05 日	受审核方代表意见： (公章) 签名：2018 年 6 月 7 日

项目号：1801-0108-IS2　　■IS

请贵方安排人员陪同审核组 6 月 15 日上午 8 点半前抵达贵方项目现场。

日期	时 间	第 1 组		第 2 组	
		受审核部门、主责条款	编号	受审核部门、主责条款	编号
6 月 15 日	08:30 ～ 12:30	1、巡视沧州市运河区水务局非农取水在线监控采购项目现场，获取 IS 管理体系的运行证据； 2、访谈项目甲方，了解项目试运行、信息安全管理要求和客户满意情况。			A
	13:00 ～ 16:30	查看项目资料，补充获取证据： IS：A.6.1.1、A.6.1.5、A.8.1.1、 A.9.2、A.11.2.5、A.11.2.6、A.11.2.9、A.12.3.1、A.16.1.2、A.16.1.3、A.18.1.3；			A
	16:30 ～ 17:00	1、和受审核方负责人沟通项目现场的审核发现。 2、结合在公司本部抽样审核的审核发现，和受审核方负责人宣布审核组的推荐结论。			A

注：1) GB/T19001-2016 标准中 4.1、4.2、5.3、6.1、6.2、7.3、10.1 在每个部门都应审核到，在审核计划中只需在主控部门列出即可(监督审核除外)。

2) 对于监督/再认证审核：除本次正常审核的内容外，还要检查上次不符合项纠正措施的验证、认证证书及标志的使用情况、体系变更情况、对组织投诉记录的调阅、资质核查及再确认等。

3）本次审核验证情况：☒无　□有，简述：

4）其他事宜：无。

不符合项、改进措施及企业整改成效证明

XQCC B210　　1997年10月首次发布　　2017年7月第17次修改

不 符 合 项 报 告

项目号：1801-0108-IS2　　第 1 项 共 7 项

审核类型	☒ IS 初审（第 2 阶段）				
发现部门	体系管理小组	陪同人员	王帅伟	审核日期	2018 年 6 月 4 日 至 5 日
审 核 准 则	☒ GB/T22080-2016 idt ISO/IEC27001:2013				
	☒ 标准条款号： IS:A.11.2.9　　□其他文件：				

不符合项事实描述(列出审核依据的相应条款及内容；需要时说明对产品和服务质量/环境/职业健康安全/食品安全/信息安全/能源绩效的影响程度)

现场查公司第一会议室笔记本电脑（ZL-33）和公司培训室台式计算机（ZL-38），未设开机密码、无屏保。两台机器中都有部门技术资料和会议记录等。

以上事实不符合 GB/T22080-2016 idt ISO/IEC27001:2013 标准 A.11.2.9 条款的相关要求。

结论：□ 严重不符合项　　☒ 轻微不符合项　　从末次会议起 30 天内完成

审核员	李华	审核组长	李华	受审核方代表	

不 符 合 项 报 告（续完）

受审核方对不符合项的处理（如下面空白处填写不下，可另附页）

项目号：**1801-0108-IS2** 第 1 项 共 7 项

1) 不符合项纠正（包括举一反三自查情况；附书面证据）：

已针对公司第一会议室笔记本电脑（ZL-38）和公司培训室台式计算机（ZL-38）进行如下纠正：

① 设置开机密码（8 位或以上，3 种字符）；

② 设置屏保（5 分钟启用，勾选“在恢复时显示登录屏幕”）；

③ 清空上述电脑桌面上文件。

第一会议室笔记本电脑（ZL-38）和公司培训室台式计算机（ZL-38）的整改后的状态见附件 1－1；

④ 针对上述情况进行举一反三， 检查其它共用笔记本和台式机有无此类情况发生，如有进行整改，检查记录见附件 1－2。

2) 原因分析：

由于相关管理人员疏忽，且对 GB/T 22080-2016 标准的 A.11.2.9 理解不透彻，导致对上述两台公共电脑的安全设置遗漏。

3) 纠正措施及实施情况（附书面证据）：

对相关人员进行 GB/T22080-2016 标准 A.11.2.9 条款和公司《AMCX13 物理区域和设备设施安全管理程序》的培训，培训记录见附件附件 1－3。

4) 纠正措施验证情况（附书面证据）：提供了培训评价，培训有效。

要求完成日期： **2018-7-5** ；实际完成日期：2018 年 6 月 19 日； 受审核方代表：李海增

注：1.初次审核的轻微不符合项宜在末次会议后 30 天内提交纠正和纠正措施完成及验证合格的证据，适用时也可以是纠正和纠正措施计划；严重不符合项应在末次会议后 60 天内提交纠正和纠正措施完成及验证合格的证据。

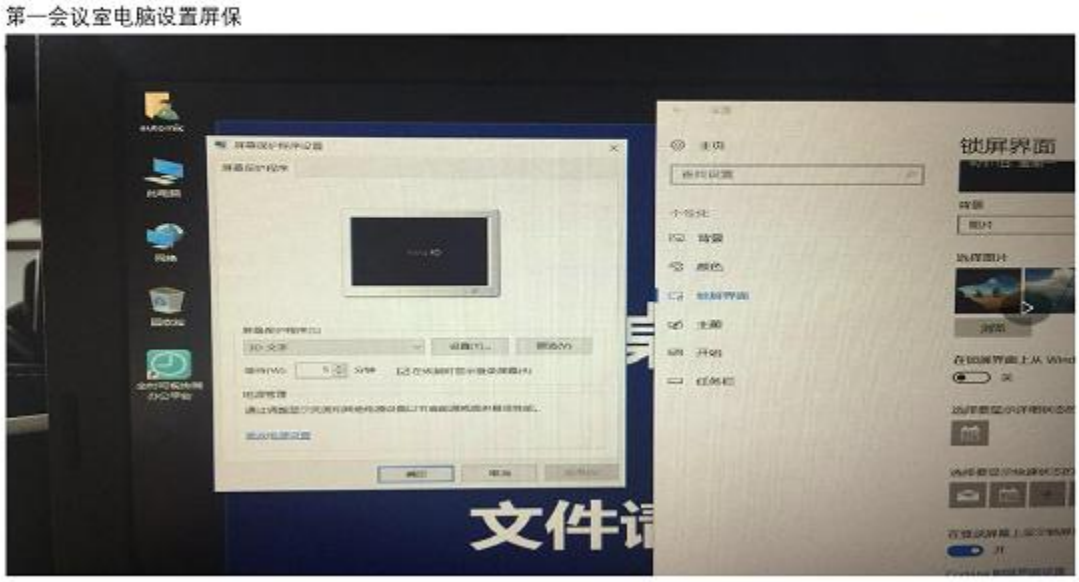
2.监督和再认证审核时产生的不符合项的关闭时间，应考虑到监督和再认证周期的要求，应确保在到期前能完成有效性验证。

附件 1 对公共电脑进行相关设置

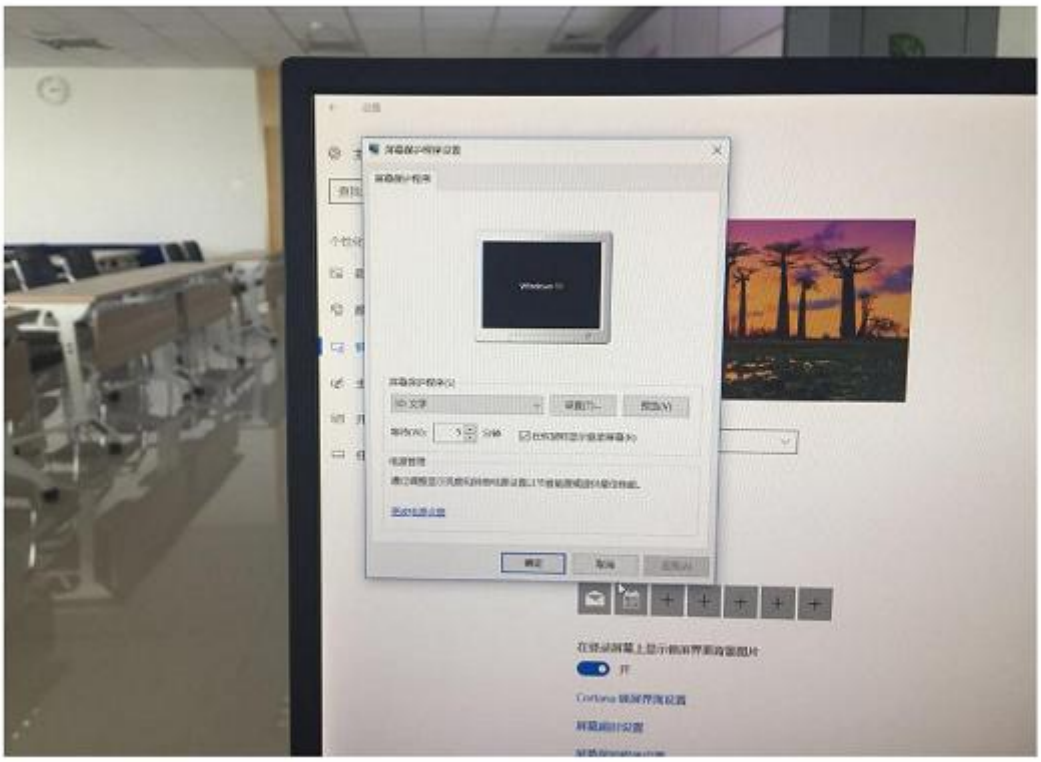
第一会议室和培训教室电脑分别增加开机密码（8 位或以上，3 种字符）

第一会议室和培训教室电脑桌面分别清空相关文件

第一会议室电脑设置屏保



培训教室电脑设置屏保



公用电脑检查表

资产编号	资产名称	开机密码位数和组成是否符合要求	是否设置屏保	桌面是否有工作文档	检查结果	备注
ZL-33	笔记本电脑	是	是	否	符合	
ZL-38	台式机电脑	是	是	否	符合	

检查人：[illegible]　　检查日期：2018.6.12

不 符 合 项 报 告

项目号：1801-0108-IS2 第 2 项 共 7 项

审核类型	☒ IS 初审（第2阶段）				
发现部门	财务中心	陪同人员	王帅伟	审核日期	2018年6月4日至5日
审核准则	☒ GB/T22080-2016 idt ISO/IEC27001:2013				
	☒ 标准条款号： IS:A.8.3.1 ☐其他文件：				

不符合项事实描述(列出审核依据的相应条款及内容；需要时说明对产品和服务质量/环境/职业健康安全/食品安全/信息安全/能源绩效的影响程度)

查见公司对U盘发放建立了办公用品发放记录，但对于使用去向追溯（比如投标交付）和使用情况缺少管理证据。

现场查见2018年3月13日吕*领取1个2G容量优盘。2018-6-5上午已用1.48G。存储了从2017年至今的公司财务文件，包括经营情况表、预算表等。吕说该优盘放在他的随身包中，经常在家办公需要使用。查公司OA系统《可移动介质授权审批表》，未见吕丹U盘记录。

以上事实不符合GB/T22080-2016 idt ISO/IEC27001:2013标准A.8.3.1条款的相关要求。不符合《AMCX08 介质和信息交换管理程序》关于“向可移动介质拷贝涉密信息，或将可移动介质带离开本公司需要获得本部门领导的批准，并在《可移动介质授权使用清单》上记录存储的信息、用途、批准人、操作人等相关信息”的管理规定。

结论：☐ 严重不符合项 ☒ 轻微不符合项 从末次会议起 30 天内完成

审核员	李华	审核组长	李华	受审核方代表	

不 符 合 项 报 告（续完）

受审核方对不符合项的处理（如下面空白处填写不下，可另附页）

项目号：**1801-0108-IS2** 第 2 项 共 7 项

1) 不符合项纠正（包括举一反三自查情况；附书面证据）：

①吕*在OA系统上补填《可移动介质授权审批表》。具体见附件2-1

②根据领取情况对吕*使用记录进行检查。检查记录见附件2-2

③根据《可移动介质授权审批表》中规定的使用期限，到期后对可移动介质进行回收。收回的记录见附件2-2

④基于以上情况进行举一反三，对办公用品发放记录进行筛查，对领用U盘的进行检查，检查记录见附件2-2。对于领用的U盘没有进行审批，一律在OA系统上补填《可移动介质授权审批表》。具体见附件2-1

2) 原因分析：

由于体系建立后在标准和文件的培训过程中，相关人员对GB/T22080:2016标准的A.8.3.1条款和公司的《AMCX08介质和信息交换管理程序》理解不透彻。

3) 纠正措施及实施情况（附书面证据）：

对GB/T22080:2016标准的A.8.3.1条款和公司的《AMCX08介质和信息交换管理程序》进行培训，培训记录见附件1-3

4) 纠正措施验证情况（附书面证据）：提供了培训评价，培训有效。

要求完成日期： 2018-7-5 ；实际完成日期：2018年6月19日； 受审核方代表：李海增

注：1.初次审核的轻微不符合项宜在末次会议后30天内提交纠正和纠正措施完成及验证合格的证据，适用时也可以是纠正和纠正措施计划；严重不符合项应在末次会议后60天内提交纠正和纠正措施完成及验证合格的证据。

2.监督和再认证审核时产生的不符合项的关闭时间，应考虑到监督和再认证周期的要求，应确保在到期前能完成有效性验证。

查询可移动介质授权审批表

表单名称:可移动介质授权审批表
查询日期:2018-06-08

移动介质名称	使用目的	使用人	使用时间	是否回收	批准人	批准时间	备注	回收人	回收时间	记录序号
U盘	会议	安弘	2018-06-08	是	杨丽丽	2018-06-08	已回收	贾美	2018-06-08	YDJZ201806006
U盘	中国水电建设集团十五工程局有限公司延安黄河引水工程管理调度系统-物联网与设施监控投标使用	孙雨晨	2018-06-08	否	吴江	2018-06-08				YDJZ201806005
u盘	张北县山洪灾害防治非工程措施2018年运行维护项目三次	李建平	2018-06-08	否	曹上智	2018-06-08				YDJZ201806004
U盘	张北县山洪灾害防治非工程措施2018年运行维护项目二次	李建平	2018-06-08	否	曹上智	2018-06-08				YDJZ201806003
U盘	会议资料	吕丹	2018-06-08	是	吕丹	2018-06-08	已回收	贾美	2018-06-08	YDJZ201806002

可移动介质使用记录检查表

检查日期:2018-06-08　　检查人：贾美

移动介质名称	使用目的	保存文件	使用人	使用时间	是否符合使用要求	存放位置	批准人	批准时间	记录序号
U盘	会议	会议资料	安弘	2018-06-08	符合	工位	杨丽丽	2018-06-08	YDJZ201806006
U盘	会议资料	会议资料、财务资料	吕丹	2018-06-08	符合	工位	吕丹	2018-06-08	YDJZ201806002
U盘	中国水电建设集团十五工程局有限公司延安黄河引水工程管理调度系统-物联网与设施监控投标使用	投标文件	孙雨晨	2018-06-08	符合	已交招标客户	吴江	2018-06-08	YDJZ201806005
u盘	张北县山洪灾害防治非工程措施2018年运行维护项目三次	投标文件	李建平	2018-06-08	符合	已交招标客户	曹上智	2018-06-08	YDJZ201806004
U盘	张北县山洪灾害防治非工程措施2018年运行维护项目二次	投标文件	李建平	2018-06-08	符合	已交招标客户	曹上智	2018-06-08	YDJZ201806003

不 符 合 项 报 告

项目号：1801-0108-IS2 第 4 项 共 7 项

审核类型	☒ IS 初审（第 2 阶段）				
发现部门	行政人事中心	陪同人员	贾美	审核日期	2018年6月4日至5日
审核准则	☒ GB/T22080-2016 idt ISO/IEC27001:2013				
	☒ 标准条款号： IS： A.12.4.3 ☐其他文件：				

不符合项事实描述(列出审核依据的相应条款及内容；需要时说明对产品和服务质量/环境/职业健康安全/食品安全/信息安全/能源绩效的影响程度)

查《AMCX16 日志管理程序》对日志定期评审没有规定。门禁系统日志管理员可以删除日志信息。

以上事实不符合 GB/T22080-2016 idt ISO/IEC27001:2013 标准 A.12.4.3 条款的相关要求。

结论：☐ 严重不符合项 ☒ 轻微不符合项 从末次会议起 30 天内完成

审核员	高玉堂	审核组长	李华	受审核方代表	

不 符 合 项 报 告（续完）

受审核方对不符合项的处理（如下面空白处填写不下，可另附页）

项目号：1801-0108-IS2 第 4 项 共 7 项

1) 不符合项纠正（包括举一反三自查情况；附书面证据）：

①对《日志管理程序》进行修订，增加对日志进行评审的要求。更改后的《日志管理程序》具体见附件 4-1

②对监控系统的日志进行检查。检查记录见附件 4-2

③ 举一反三自查，对公司的所有信息系统的日志进行检查，检查记录见附件 4-2

2) 原因分析：

由于体系建立后在标准和文件的培训过程中，相关人员对 GB/T22080:2016 标准的 A.12.4.3 条款理解不透彻。

3) 纠正措施及实施情况（附书面证据）：

对相关人员进行 GB/T22080:2016 标准的 A.12.4.3 条款进行培训，培训记录见附件 1－3。

4) 纠正措施验证情况（附书面证据）：提供了培训评价，培训有效。

要求完成日期： 2018-7-5 ；实际完成日期：2018 年 6 月 19 日； 受审核方代表：李海增

注：1.初次审核的轻微不符合项宜在末次会议后 30 天内提交纠正和纠正措施完成及验证合格的证据，适用时也可以是纠正和纠正措施计划；严重不符合项应在末次会议后 60 天内提交纠正和纠正措施完成及验证合格的证据。

2.监督和再认证审核时产生的不符合项的关闭时间，应考虑到监督和再认证周期的要求，应确保在到期前能完成有效性验证。

文件编号：AM--CX-16

密级：秘密

奥特美克

日志管理程序

版本号：V1.1.0

北京奥特美克科技股份有限公司

1

历史版本信息

审批记录

版本	日期	审核	会签	批准	编写部门
V1.0.0	2017.9.25	贾美	贾美、张恩	李海增	信息化部
V1.1.0	2018.6.8	贾美	贾美、张恩、张明	李海增	信息化部

修订记录

日期	修订版本	描述	修订人	备注
2018.6.8	V1.1.0	增加对日志进行定期评审的要求	贾美	

目录

1 目的

建立一个标准化的信息处理活动的记录和跟踪体系，以支持未来的调查和访问控制监控。

2 范围

本程序适用于本公司信息安全管理体系（ISMS）所覆盖的所有部门信息处理活动。

3 定义

无

4 职责

4.1 各系统、设备管理人员

应按本程序的规定保存、备份、记录处理日志。

5 内容

5.1 设备、系统的日志配置

开启信息设备、系统的审计日志记录功能。

4.1.1 UTM（Unified Threat Management）设备日志记录配置：

UTM 设备开启日志如下：

（1） 事件日志：记录日期、事件和事件内容。记录尝试访问防火墙的账户和 IP。如登陆和退出。

（2） 告警日志：记录防火墙告警信息，如防火墙重启信息。

（3） 安全日志：记录防火墙所拦截的外网攻击以及内网通过防火墙流量的攻击行为信息。

（4） 配置日志：记录防火墙配置调整信息。

（5） 网络日志：记录通过防火墙的数据的来源 IP 地址和协议及数据包的发送状态等信息。

4.1.2 操作系统日志记录配置：

（1） windows 操作系统日志记录采用系统默认配置。

开启项为：应用程序、安全、setup、系统、转发事件。

（2）linux 操作系统日志记录采用系统默认配置。

开启项为：

1） Message：记录系统启动后的信息和错误日志信息。

2） secure：记录与安全相关的日志信息。

3） maillog：记录与邮件相关的日志信息。

4) cron：记录与定时任务相关的日志信息。

5) spooler：记录与 UUCP 和 NEWS 设备相关的日志信息。

6) boot：记录守护进程启动和停止相关的日志消息。

日志存储路径为/var/log。

5.2 日志的备份和保护

为了防止日志文件被未授权人清空或篡改应该对日志文件进行保护。方法是：

a) windows 操作系统修改日志文件默认存放目录，将默认存放目录设置为非系统盘下。

b) 日志应至少保存 6 个月，对于不能保存 6 个月的日志，应定期进行备份。

5.3 管理员和操作员的活动日志

a) 系统管理员和操作员在对设备进行操作和维护时须登记，填写《信息系统和设备操作记录单》。

b) 设备自身有记录管理员操作日志功能的需启用，并对日志进行保存。

5.4 故障日志

防火墙，交换机，服务器等重要设备出现故障必须将故障发生的时间，故障描述以及分析过程、处理措施和处理结果等记录在《故障日志处理记录》中。

5.5 日志的评审

各信息系统管理部门负责人每月应对系统日志是否完整，保存期限是否符合要求，是否被篡改进行检查。填写《系统日志检查记录单》。

6 相关文件

《信息资产识别和信息安全风险管理程序》

7 相关记录

序号	记录编号	记录名称	使用部门	保存部门	保存期限
1	JL-CX/16-01	《故障日志处理记录》	各部门	各部门	3 年
2	JL-CX/14-02	《信息系统和设备操作记录单》	各部门	各部门	3 年
3	JL-CX/14-03	《系统日志检查记录单》	各部门	各部门	3 年

系统日志检查记录单

编号：JL-CX/14-03

系统名称	日志是否完整	日志保存期限是否符合要求	日志是否被篡改	检查人	检查日期	备注
SVN	是	是	否	李晓	2018.6.15	
redmine	是	是	否	呼唤	2018.6.15	
Mantis	是	是	否	呼唤	2018.6.15	

注：检查人应该是部门负责人，每月检查一次。

系统日志检查记录单

编号：JL-CX/14-03

系统名称	日志是否完整	日志保存期限是否符合要求	日志是否被篡改	检查人	检查日期	备注
监控系统	是	是	无	张恩	2018.06.12	
U8	是	是	无	张恩	2018.06.12	
OA	是	是	无	张恩	2018.06.12	
档案管理系统	是	是	无	张恩	2018.06.12	

注：检查人应该是部门负责人，每月检查一次。

不 符 合 项 报 告

项目号：1801-0108-IS2 第 7 项 共 7 项

审核类型	☒ IS 初审（第 2 阶段）				
发现部门	客服中心	陪同人员	任建国	审核日期	2018 年 6 月 5 日
审核准则	☒ GB/T22080-2016 idt ISO/IEC27001:2013				
	☒ 标准条款号： IS： A.6.1.5 ☐其他文件：				

不符合项事实描述(列出审核依据的相应条款及内容；需要时说明对产品和服务质量/环境/职业健康安全/食品安全/信息安全/能源绩效的影响程度)

客服中心租用上海新道仓信息科技有限公司开发 SaaS（软件即服务）平台类软件“北京奥特美克运维服务管理系统”，用于运维项目管理。对其数据存放地理位置、安全防护措施未做明确要求；现场登录系统，发现工单上有客户的姓名和联系电话等敏感信息显示，未见识别和防护证据。

以上事实不符合 GB/T22080-2016 idt ISO/IEC27001:2013 标准附录 A 中 A.6.1.5 条款的相关要求。

结论：☐ 严重不符合项 ☒ 轻微不符合项 从末次会议起 30 天内完成

审核员		审核组长	李华	受审核方代表	

不 符 合 项 报 告（续完）

受审核方对不符合项的处理（如下面空白处填写不下，可另附页）

项目号：1801-0108-IS2 第 7 项 共 7 项

1) 不符合项纠正（包括举一反三自查情况；附书面证据）：

①公司与“上海新道仑信息科技有限公司”签订《保密协议》，明确公司在租用软件期间产生的所有数据，无论是存贮在物理服务器或是云上，都应永久保密，并采取安全措施以防泄露的要求，以及要求出租方定期对数据进行备份以防数据丢失的要求。签订的《保密协议》见附件 7－1

②在《部门信息资产识别表》中增加“客户信息”、租用的软件和软件租赁方，增加后的《部门信息资产识别表》见附件 7－2

③举一反三自查，检查本部门在运维过程中产生的数据和信息有无无安全防护和泄露风险，检查记录见附件 7－3

2) 原因分析：

由于体系建立后在标准和文件的过程中，相关人员对 GB/T22080-2016 标准的 A.6.1.5 条款理解不透彻。

3) 纠正措施及实施情况（附书面证据）：

对相关人员进行 GB/T22080-2016 标准的 A.6.1.5 条款的培训，培训记录见附件

4) 纠正措施验证情况（附书面证据）：提供了培训评价，培训有效。

要求完成日期： 2018-7-5 ；实际完成日期：2018 年 6 月 19 日； 受审核方代表：李海增

注：1.初次审核的轻微不符合项宜在末次会议后 30 天内提交纠正和纠正措施完成及验证合格的证据，适用时也可以是纠正和纠正措施计划；严重不符合项应在末次会议后 60 天内提交纠正和纠正措施完成及验证合格的证据。

2.监督和再认证审核时产生的不符合项的关闭时间，应考虑到监督和再认证周期的要求，应确保在到期前能完成有效性验证。

信息安全保密协议

甲方：北京奥特美克科技股份有限公司
地址： 北京市海淀区西北旺东路 10 号院东区 5 号楼 6 层 601-1
负责人：刘钊
乙方： 上海新道仑信息科技有限公司
地址： 上海市嘉定区德富路 1090 号宝龙广场 5 号楼 1308 室
负责人： 熊军民

鉴于：

1、甲方向乙方租用：道仑售后服务管理系统（标准版）（以下简称“道仑软件”）。

2、在软件租用过程中，甲方已经或将要向乙方提供或披露（或乙方可能获悉）甲方的某些秘密性、专有性或保密性信息（“保密信息”），且该保密信息属甲方合法所有或掌握。

3、双方均对本协议所述保密信息予以有效保护。

经双方协商，达成本协议。

第一条 保密信息

1.1 保密信息包括但不限于以下内容：甲方客户信息、甲方产品信息、甲方设备及项目信息、甲方服务信息等；

1.2 上述保密信息可以以数据、文字及记载上述内容的文档、光盘、软件、图书等有形介质体现，也可通过口头等视听方式传递。

第二条 数据信息安全

2.1 鉴于软件租用形式，乙方将软件发布在阿里云华东 2 上海机房，部署服务器编号：i-uf63cbiz72g5mujfn6mg。

2.2 乙方每月初（每月五日前）以邮件形式提供上月系统所属业务数据（含主数据）备份。甲方备份数据接收人：刘钊 接收邮箱：liuzhao@automic.com.cn。

2.3 乙方确保在软件租用期间的数据信息安全。对于可能发生数据信息安全事件，按租用协议相关条款进行处理。

第三条 双方权利和义务

3.1 乙方保证该保密信息仅用于租用系统使用有关的用途，乙方不

得将保密信息用于除此以外的任何用途。

3.2 乙方保证对保密信息予以妥善保管，并对保密信息在乙方期间发生的以下事项承担全部责任，因此造成甲方损失的，乙方应负责赔偿。

3.3 乙方保证对保密信息按本协议约定予以保密，并至少采取不低于对乙方保密信息的保护手段进行保密。

3.4 乙方如发现保密信息泄露，应采取有效措施防止泄密进一步扩大，并及时告知甲方。

3.5 软件租用终止后，乙方应及时将保密信息全部清除、销毁或返还甲方。

3.6 上述限制条款不适用于以下情况：

3.6.1 在依本协议披露之时，该保密信息已以合法方式属乙方所有或由乙方知悉。

3.6.2 在依本协议披露之时，该保密信息已经公开或能从公开领域获得。

3.6.3 保密信息是乙方从没有违反对甲方保密或不披露义务的人合法取得的。

3.6.4 该保密信息是乙方或其关联或附属公司独立开发，而且未从甲方或其关联或附属公司披露或提供的信息中获益。

3.6.5 经甲方书面同意对外披露，但仅限于甲方书面同意的范围、方式且遵循书面同意中规定的其他前提条件。

3.6.6 乙方应法律、行政法规要求披露的信息（通过口头提问、询问、要求资料或文件、传唤、民事或刑事调查或其他程序披露保密信息）。

3.7 如果乙方拟以本协议第 3.6.5 条、第 3.6.6 条为依据作出披露的，应至少于实际作出披露行为前五个工作日通知甲方，说明其拟根据上述约定披露有关的保密信息，并就披露对象和披露范围、方式等作出说明。

3.8 甲方不保证保密信息的精确性与合理性。

3.9 如果乙方得知第三方获得任何保密信息，则应及时书面通知甲方，并向甲方提供掌握的所有相关情况。

3.10 双方一致认同，对于本协议签订及履行过程中、项目的商谈及合作过程中所接触到的甲方关联公司的保密信息，乙方并应依据本协议约定履行保密义务、承担责任。

第四条 违约责任

乙方未履行或未完全履行本协议项下的条款均构成违约乙方应赔偿因此而给甲方造成的一切损失，包括但不限于甲方因调查违约行为而支付的合理费用。

第无条 甲方在履行本协议的任何条款时，如有放松、放弃或迟延，均不构成对甲方在本协议下任何权利的不利影响或限制。如果甲方对某一违约行为免予追究，并不构成放弃追究乙方随后或持续违约行为的权利。

第六条 法律适用和争议解决

6.1 本协议适用中华人民共和国法律。

6.2 所有因本协议引起的或与本协议有关的任何争议将通过双方友好协商解决。如果双方不能通过友好协商解决争议，则任何一方均可采取下述争议解决方式：

（1）将该争议提交至甲方注册地址所在仲裁委员会，按照申请仲裁时该会的仲裁规则进行仲裁。仲裁在甲方注册地址进行。仲裁语言为中文。仲裁裁决是终局的，对双方均有约束力。仲裁费用由败诉方承担。

6.3 仲裁进行过程中，双方将继续履行本协议未涉仲裁的其它部分。

第七条 协议生效及其他

7.1 本协议自双方于 2018 年 4 月 28 日签字盖章之日起生效。有效期为双方租用协议的有效期限或提供平台维护、技术支撑的有效期限。本协议签署前，甲方已经向乙方提供或披露的本协议范围内的保密信息也受本协议约束，此时本协议于该等保密信息提供或披露时发生效力。

7.2 本协议一式肆份，甲乙双方各执贰份，具有同等法律效力。

7.3 如果本协议的任何条款在任何时候变成不合法、无效或不可强制执行而不从根本上影响本协议的效力时，本协议的其它条款不受影响。

7.4 本协议各条标题仅为提示之用，应以条文内容确定各方的权利义务。

7.5 本协议替代此前双方所有关于本协议事项的口头或书面的纪要、备忘录、合同和协议。

7.6 对协议内容做出的任何修改和补充应为书面形式，由双方签字盖章后成为协议不可分割的部分。

7.7 双方因履行本协议或与本协议有关的一切通知都必须按照本协

议中的地址，以书面信函形式或双方确认的传真或类似的通讯方式进行。采用信函方式的应使用挂号信或者具有良好信誉的特快专递送达。如使用传真或类似的通讯方式，通知日期即为通讯发出日期，如使用挂号信件或特快专递，通知日期即为邮件寄出日期并以邮戳为准。

甲方：北京奥特美克科技股份有限公司

地　址：北京市海淀区西北旺东路10号院东区5号楼6层601-1

联系人：刘钊

电　话：18600476105

传　真：010-82894252

邮　编：

乙方：上海新道仑信息科技有限公司

地　址：上海市嘉定区德富路1090号宝龙广场5号楼1308室

联系人：曹云华

电　话：021-60712966

传　真：

邮　编：

甲方：北京奥特美克科技股份有限公司

法定代表人

或授权代表（签字）：

2018年6月8日

乙方：上海新道仑信息科技有限公司

法定代表人

或授权代表（签字）：

2018年6月8日

服务

编号：JL-CX/06-01

序号	服务商名称	提供的服务内容	责任人	C
1	上海新道仓信息科技有限公司	运维服务管理系统租赁	刘钊	4

资产赋值		资产值
I	A	
3	3	4

客服中心保密信息安全检查记录单

保密信息	存放位置	是否存在泄露风险	是否有备份	备注
项目预算表	李建平： D:\LJP\我的工作	否	是	/
项目过程资料	项目工程师电脑： 个人电脑 E：\项目资料	否	是	/
项目监理文档	项目工程师电脑： 个人电脑 E：\项目资料	否	是	/
客户信息	https://www.xtaoroad.com/tomis	否	是	/

检查人：刘伟 检查时间：2018.6.12

员工培训记录及有效性评价

时间	2018.6.8	培训老师	霍老师	培训方式	面授
地点	一会议室	培训对象	财务中心、质量管理部、客服中心、研发中心、行政人事中心相关人员、体系管理小组	考核方式	提问

培训内容：外审不符合项纠正措施涉及的内容

参加培训人员签到及成绩单：

部门	签到	成绩	部门	签到	成绩
财务			营销		
客服中心			信息化		
			研发中心		
信息化			质量管理部		
行政			供方链中心		
人事			财务		
研发中心					
规划设计院					
运营					
营销中心					

培训简况（包括内容、教材等）：

1、GB/T 22080-2016标准的A.6.1.5、A.8.3.1、A.9.2.2、A.9.2.3、A.9.2.5、A.11.2.8、A.11.2.9、A.12.4.3、A.12.4.4

2、公司的《物理区域和设备设施安全管理程序》、《介质和信息交换管理程序》、《用户访问管理程序》

培训效果评价：

参加培训人员认真听讲，积极回答问题，互动良好提问，确认参加培训人员掌握了培训内容。

培训结论：

本次培训合格

评价参加人员	部门	评价参加人员	部门

不符合项整改相关内容发布至公司 OA 讨论区，供大家参考学习。

观察项报告

项目号：1801-0108-IS2

审核时间：2018 年 6 月 4 日至 5 日　　审核类型：IS：初审(第 2 阶段)

序号	事 实 描 述	标准条款
1.	公司《部门职责说明书》，宜明确描述信息安全风险识别、信息安全事件和人员授权等管理职责。	5.3
2.	公司宜关注风险评估中对人员、该人员使用和管理的信息处理设施、文档、数据等资产“CIA”赋值的一致性。	6.1.2
3.	公司宜在运维活动中完善项目的信息安全工作，包括进行安全风险评估、甲方信息系统远程访问权控制、运维团队信息安全技术培训等。	A.6.1.5
4.	公司应关注特殊岗位入职人员背景核查。	A.7.1.1
5.	宜完善财务办公室的公章、现金柜、文件柜、U 盘等资产识别和管理责任人。 宜加强部门所使用软件和系统的识别与权限控制。	A.8.1.1
6.	宜保持文件描述一致性，比如：《AMCX12 涉密信息的分级处理管理程序》与《适用性声明》对信息密级分类；机房设备标签上的密级标记。	A.8.2.1 A.8.2.2
7.	公司宜整体策划全国范围内在建、在用的水资源信息系统的远程技术支持的访问控制策略。	A.9.1.1
8.	宜对机房空调的运行建立有效监控手段。	A.11.2.2
9.	宜加强个人电脑上软件安装的控制。宜加强个人电脑杀毒软件的更新控制	A.12.2.1
10.	公司应关注对新购系统、开源系统需求信息的规范管理。 宜加强外购的自用信息系统的安全管理要求。	A.14.1.1
11.	公司应加强对信息安全相关供应商（含研发中心测试、系统服务）的全面识别和管理。	A.15
12.	公司宜完善《AMCX18 信息安全事件管理程序》指引的应急管理程序。	A.16.1.5
13.	宜在《信息安全日常巡检表》完善检查的具体可追溯信息。	A.16.1.7

第 1 页 共 1 页　　审核员（签字）：王玉志 李华 高玉堂

观察项报告

项目号：1801-0108-IS2

审核时间：2018 年 6 月 15 日　　审核类型：IS：初审(第 2 阶段)项目现场

序号	事 实 描 述	标准条款
1.	应关注《施工组织方案》项目人员岗位职责中信息安全管理内容的完善性，并在施工安全文明交底中强调信息安全管理要求。	A.6.1.5
2.	在 3 个设备安装现场均看到 220 伏市电供电不连接，建议在施工日志或安装调试记录中记录该类实际情况。	A.18.1.3

第 1 页 共 1 页　　审核员（签字）：李华